DTCC Terms for SEC Regulation S-P

Updated: November 24, 2025

DTCC, through its affiliates National Securities Clearing Corporation ("NSCC"), The Depository Trust Company ("DTC"), the Fixed Income Clearing Corporation ("FICC"), and DTCC Institutional Trade Processing ("ITP") (collectively, "DTCC"), provide services to entities that are subject to SEC Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information, 15 CFR part 248 ("Reg S-P"), in which the services provided contain "Customer Information" as defined under the regulation. DTCC recognizes that Reg S-P requires entities subject to it ("Covered Institutions") to have incident response programs that would, among other things, include policies and procedures reasonably designed to ensure service providers take appropriate measures to protect against unauthorized access to or use of customer information and provide notification to the covered institution of certain incidents within the timeframe specified in the regulation.

DTCC maintains written policies and procedures reasonably designed to protect sensitive personal information, including customer information, against both internal and external threats. Policies and procedures have been implemented to address administrative, technical, and physical safeguards and include:

- Requirements for establishing, implementing, maintaining, and continually improving an information risk management program
- A governance structure utilized for the escalation of information risks to an appropriate management level
- Organizational roles and responsibilities for the delivery of a comprehensive information security and technology risk management program

Additionally, all data must be appropriately classified, which determines the sensitivity of the data and the associated controls. Customer data is encrypted in transit and at rest using encryption levels appropriate to the risk and sensitivity of the data. Layered controls are in place, including firewalls, encryption, and access management. Personnel undergo background checks and training is provided both at onboarding and ongoing. User access management controls are in place to prevent unauthorized access and access to customer data is restricted to personnel who require access as part of their job responsibilities. All personnel have unique login credentials and access is logged.

DTCC performs risk assessments throughout the year, which include internal and third-party network scans, reviews for sufficient network, storage, and compute capacity needs. Controls are tested to confirm they function as intended. The monitoring and management of incidents are subject to written policies and procedures, and include monitoring of systems, detection of unauthorized information processing activities, analyzing of any potential threats, response actions to be taken in the event of unauthorized access, and internal and external incident reporting. Incident response tabletop exercises are conducted periodically to maintain proficiency. As a service provider, DTCC maintains procedures to notify impacted parties within applicable regulatory requirements, such as within 72 hours under Reg S-P, after becoming aware that a breach of security has occurred resulting in unauthorized access to customer information.